Modelo de procedimiento sancionador electrónico aplicado al control del tráfico vehicular

J. M. de Fuentes, A. I. González-Tablas, A. Ribagorda
Grupo de Seguridad en las T.I.C. Universidad Carlos III de Madrid (España)
Email: {jfuentes,aigonzal,arturo}@inf.uc3m.es

***Resumen*—El incumplimiento de las leyes origina la imposición de sanciones. Una buena gestión de las sanciones se convierte en un factor clave para que éstas sean eficaces. Por este motivo, se han producido impulsos legislativos que persiguen el desarrollo electrónico de los procedimientos. No obstante, hasta el momento no se ha propuesto la realización electrónica del procedimiento sancionador completo en el ámbito del control del tráfico vehicular. En este trabajo se propone un modelo para la implantación del procedimiento sancionador electrónico en dicho contexto, mejorando la capacidad de participación de los ciudadanos interesados en el mismo. Particularmente y por las implicaciones legales del procedimiento, se abordan en detalle los aspectos de seguridad necesarios.**

***Palabras clave:* Procedimiento sancionador electrónico, tráfico, sanción, seguridad.**

I. Introducción

A través de la legislación, los estados determinan qué actuaciones están permitidas dentro de su territorio. El incumplimiento de las leyes lleva consigo la imposición de una sanción, que debe ser proporcionada y justa. Para garantizar la observancia de estos principios, se ha definido un procedimiento específico para el establecimiento de las sanciones.

El procedimiento sancionador abarca todo el ciclo de gestión de la sanción, desde la observación del mal cometido hasta que se establece definitivamente la sanción correspondiente. Actualmente, dicho ciclo lleva asociada una notable carga burocrática. Esto origina una gran cantidad de documentación y, al mismo tiempo, la dilatación en el tiempo de los procedimientos. Ambas cuestiones han desembocado en una gestión ineficiente de las sanciones, provocando incluso que haya procedimientos que caduquen sin haberse establecido una sanción.

Los impulsos recientes para la agilización de la Administración Pública tienen por objetivo paliar estos defectos en la ejecución de los procedimientos. En España, esta voluntad se materializó en la Ley 11/2007, de acceso electrónico de los ciudadanos a las Administraciones Públicas [1]. Dicha Ley especifica, entre otras cuestiones, las directrices para la gestión electrónica de procedimientos administrativos.

Uno de los ámbitos donde se gestionan un mayor número de procedimientos administrativos es el control del tráfico vehicular (4,7 millones de procedimientos en 2008[1]). A la vista del elevado volumen de tramitación, la adopción de medios electrónicos (con sus beneficios previstos de transparencia, eficacia y eficiencia) se hace especialmente necesaria. Hasta el momento, sin embargo, no existen propuestas que aborden de manera electrónica todas las fases del procedimiento. Además, las contribuciones que abordan parcialmente este proceso no explotan las ventajas que brinda el desarrollo actual de las tecnologías de la información y que permitiría la interacción en tiempo real con el sancionado y los demás interesados en el procedimiento.

El objetivo de este trabajo es proponer un nuevo modelo de procedimiento sancionador electrónico aplicado al control del tráfico. Dicho modelo abarca todas las fases del proceso, promoviendo la participación directa de los interesados en ellas. Además, el modelo respeta las directrices establecidas por la citada Ley 11/2007, prestando especial atención a los aspectos de seguridad.

I-A. Organización del trabajo

La Sección II describe el proceso sancionador y presenta las normas específicas de gestión electrónica de procedimientos según la Ley 11/2007, con especial atención a las cuestiones de seguridad que ésta plantea. En la Sección III se presentan los principales antecedentes para la realización electrónica del procedimiento. La Sección IV describe el modelo propuesto, analizando sus aspectos de seguridad y presentando un análisis preliminar de la viabilidad técnica del mismo. La Sección V presenta los trabajos relacionados y, finalmente, la Sección VI recoge las principales conclusiones y líneas de trabajo futuro.

II. El procedimiento sancionador en España. Realización electrónica

El objetivo de este trabajo es mejorar el procedimiento por el cual se establecen sanciones administrativas en un ámbito concreto (el control del tráfico). En esta Sección se describe dicho procedimiento y las consideraciones de seguridad previstas en la Ley 11/2007.

II-A. Descripción del procedimiento sancionador

El procedimiento sancionador queda originalmente definido en España en la Ley 30/1992 [2]. Sin embargo, la Ley 11/2007 supuso una renovación significativa del mismo, al proponer su realización electrónica a través de las tecnologías de la información. De hecho, dicha Ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos [1]. Con ello, se pretende mejorar su transparencia, su eficacia y su accesibilidad para los ciudadanos.

[1] http://www.dgt.es/portal/es/seguridad_vial/estadistica

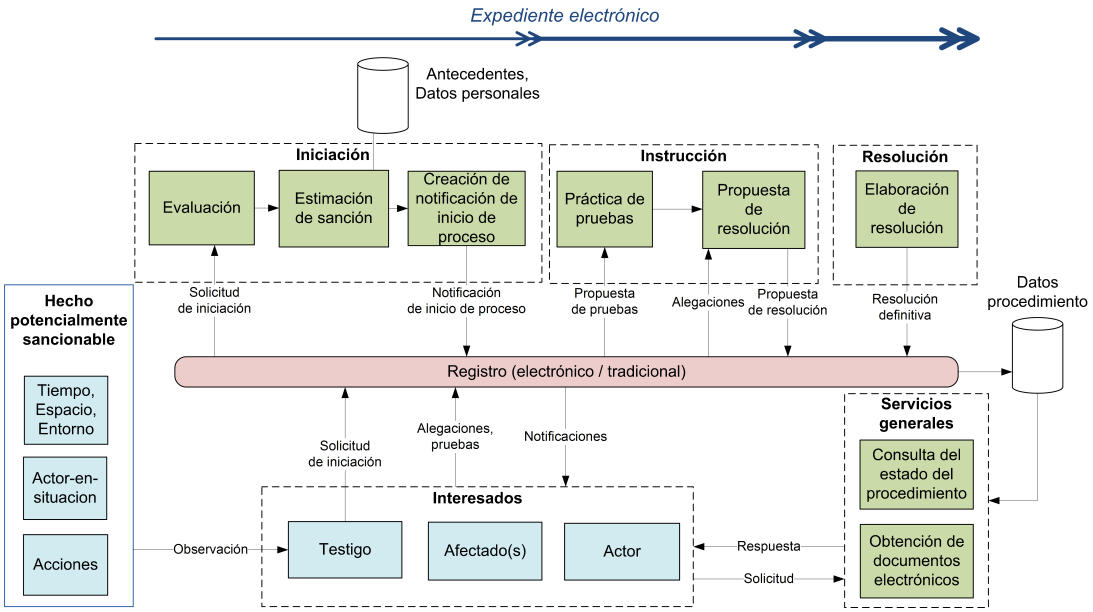

Figura 1. Procedimiento sancionador actual

La Figura 1 describe los diferentes elementos que intervienen en el procedimiento sancionador, incluyendo los medios electrónicos que la citada Ley 11/2007 contempla para su realización. Dicho procedimiento se compone de tres fases (Figura 1, arriba): iniciación, instrucción y resolución.

La fase de *iniciación* puede ser comenzada por cualquier testigo del hecho, presentando una solicitud a través de un registro. Esta presentación puede realizarse de forma electrónica a través de un registro (electrónico), aportando la copia digitalizada de los documentos que en su caso acompañen a la solicitud. Una vez recibida, la solicitud se evalúa, aceptándola o rechazándola en función de los hechos descritos. En el caso de que se acepte, se obtienen los antecedentes y datos personales que serán necesarios para establecer la sanción. Una vez se ha establecido la sanción correspondiente (siempre bajo el supuesto de que los hechos fueran ciertos), se crea la notificación de la iniciación del proceso. Esta notificación se envía a la dirección postal del implicado, salvo que el ciudadano haya permitido el envío a través de medios electrónicos, en cuyo caso así se procede.

Tras la fase de iniciación comienza la de *instrucción*. En ella los interesados pueden formular alegaciones o proponer la práctica de pruebas que permitan adecuar la sanción a la gravedad de los hechos. Así, se puede presentar el testimonio de otras personas presentes en el suceso (alegación) o proponer una pericia técnica sobre el funcionamiento de un dispositivo (prueba). Esta presentación se puede realizar a través del registro electrónico. Tras la valoración de los resultados arrojados por las alegaciones y las pruebas, el organismo instructor efectúa una propuesta de resolución que es nuevamente enviada a los interesados.

Una vez finalizada la instrucción, un organismo distinto del instructor se encarga de la *resolución*, en el que se valora la propuesta de resolución y se redacta la resolución definitiva que pone fin al proceso sancionador.

La tramitación electrónica da lugar a dos nuevos servicios adicionales para el ciudadano relacionados con el procedimiento (Figura 1, derecha). Por un lado, el ciudadano puede consultar electrónicamente los actos de trámite (incluyendo su contenido) y la fecha en que se hicieron. Por otro, el ciudadano puede obtener copias electrónicas de los documentos electrónicos que ya formen parte del procedimiento.

II-B. Necesidades de seguridad para la realización electrónica del procedimiento sancionador según la Ley 11/2007

Para la ejecución electrónica del procedimiento, la Ley contempla una serie de mecanismos técnicos y, sobre éstos, establece ciertas necesidades de seguridad. En este apartado se revisan estas cuestiones, que afectan a dos aspectos distintos: la información del procedimiento y a las relaciones con el ciudadano.

En cuanto a la información del procedimiento, se recoge en el *expediente electrónico*, que contiene *documentos administrativos electrónicos*. Ambos elementos están firmados electrónicamente, a fin de asegurar su integridad e identificar fehacientemente el órgano responsable. Los documentos deben contener, además, una referencia temporal que se presume confiable. Toda esta información se deben almacenar en un *archivo electrónico*, al cual se le exige que proteja la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos guardados. Igualmente, se impone el uso de mecanismos de control de accesos y, en general, que se satisfaga lo dispuesto en la legislación de protección de datos personales.

En cuanto a las relaciones con el ciudadano, se distinguen dos elementos: los registros y la comunicación electrónica. Los registros electrónicos se encargan de recibir y enviar todos

los documentos, escritos y solicitudes que tengan lugar en un determinado procedimiento. Dichos registros deben tener plena disponibilidad. Además, por cada documento aportado por el ciudadano, el registro debe emitir un recibo acreditativo. Dicho recibo consiste en una copia autenticada de lo aportado, incluyendo la fecha y hora de presentación y el número de entrada en el registro.

Finalmente, en la comunicación electrónica con el ciudadano debe quedar constancia de la transmisión y recepción, de sus fechas y del contenido íntegro comunicado. Así mismo, debe identificarse fidedignamente al remitente y al destinatario. Si en esa comunicación se envía una notificación electrónica, debe reflejarse la fecha y hora de la puesta a disposición del interesado de lo notificado, así como la de acceso a su contenido. Los medios empleados para este fin deberán asegurar su disponibilidad, a fin de garantizar el acceso de los ciudadanos a los procedimientos.

III. Antecedentes de tramitación electrónica de sanciones de tráfico con la participación del vehículo

Las redes vehiculares, habitualmente referidas como VANET (del inglés *Vehicular Ad-hoc NETwork*) son un tipo específico de red móvil de comunicación [3]. A través de estas redes los vehículos intercambian datos entre sí y con sistemas externos. Dichos intercambios de información permiten construir nuevos servicios electrónicos, denominados *Sistemas Inteligentes de Transporte* (SIT). Éstos se definen como "*aplicaciones avanzadas que, sin incluir la inteligencia como tal, proporcionan servicios innovadores en los modos de transporte y la gestión del tráfico y permiten a los distintos usuarios estar mejor informados y hacer un uso más seguro, más coordinado y "más inteligente"de las redes de transporte*" [4]. El procedimiento sancionador electrónico presenta dos importantes similitudes con la definición anterior: ambas cuestiones persiguen promover un uso más seguro de las carreteras y, además, buscan ofrecer una mejor información al conductor. En el caso del procedimiento sancionador, la información se refiere al estado de tramitación del procedimiento, cuestión que hasta el momento no ha sido resuelta de forma eficaz en el ámbito vehicular.

El creciente desarrollo de los citados SIT ha dado origen a una arquitectura europea de referencia para estos servicios [5]. Ésta pretende ser el marco común en el que se puedan integrar todos los SIT que se diseñen en un lugar de Europa, asegurando que se pueda incorporar en cualquier otro país de la Unión. Uno de los servicios que se aborda en esta arquitectura es, precisamente, el procedimiento sancionador electrónico. Sin embargo, la funcionalidad prevista sobre este procedimiento se limita a la fase de iniciación. De hecho, la notificación de inicio de procedimiento no se envía a través de medios electrónicos. Dado que se aborda sólo una parte del procedimiento, se disminuye la eficacia y eficiencia esperables del uso de las tecnologías de la información. Por tanto, todavía es necesario proponer contribuciones que permitan realizar el procedimiento sancionador electrónico de forma completa.

IV. Propuesta de aplicación del procedimiento sancionador electrónico al ámbito del control del tráfico

El contexto vehicular está sufriendo una profunda transformación, incorporando las tecnologías de la información en su funcionamiento rutinario. Así, el vehículo y el conductor pueden intercambiar información desde y hacia el exterior. En este trabajo se propone un modelo que abarque todas las fases del proceso sancionador aprovechando el desarrollo de las tecnologías de la información en este contexto. Dicho modelo se basa en el procedimiento sancionador descrito en la Sección II y extiende la funcionalidad prevista en la arquitectura de referencia SIT introducida en la Sección III.

El modelo que se propone tiene dos objetivos principales. El primero es alcanzar una comunicación directa con el interesado, permitiendo que el conductor tenga conocimiento inmediato del estado del procedimiento. El segundo es que el propio interesado pueda crear (y enviar a la Autoridad) pruebas electrónicas que sirvan de base para las alegaciones dentro de la fase de instrucción. Con ello se consigue que el interesado tengan una mayor capacidad de intervención en el proceso.

En esta Sección se describe en primer lugar el modelo propuesto. En el segundo apartado se abordan sus necesidades de seguridad. Finalmente, el último apartado presenta un análisis preliminar de las técnicas de interés para desarrollar la arquitectura derivada de este modelo.

IV-A. Descripción del modelo propuesto

La Figura 2 refleja el modelo propuesto expresado con un diagrama de componentes UML que refleja los cuatro subsistemas que se proponen para realizar el procedimiento sancionador electrónico. Cada subsistema aborda el procesamiento que efectúan cada una de las entidades o infraestructuras implicadas en el procedimiento, esto es, el testigo o testigos, la autoridad o autoridades, los interesados y las infraestructuras de comunicación. A continuación se explica cómo interviene cada uno de los componentes en el proceso resaltando las contribuciones que se realizan para llevar a cabo los objetivos planteados.

El proceso comienza con la detección del comportamiento potencialmente sancionable. Para ello, el Registro de datos sensoriales del testigo muestrea el entorno en busca de actuaciones ilegales. Cuando esto se produce, se emplea el componente de Acreditación y envío para que éste dote de legitimidad a los datos recogidos y se los comunique al organismo iniciador. Dicho envío se realiza a través de la Comunicación hacia la Autoridad y es recibido por su Registro electrónico. Gracias al registro, la solicitud pasa a formar parte de un nuevo expediente electrónico, de lo cual se deja constancia en la infraestructura de almacenamiento a través del componente Gestión de datos. El expediente creado se envía al componente de Iniciación, el cual evalúa lo sucedido y, en base a los antecedentes del infractor (si ha sido identificado) o del titular del vehículo (si el infractor real no ha sido identificado), establece una sanción y envía la notificación correspondiente.

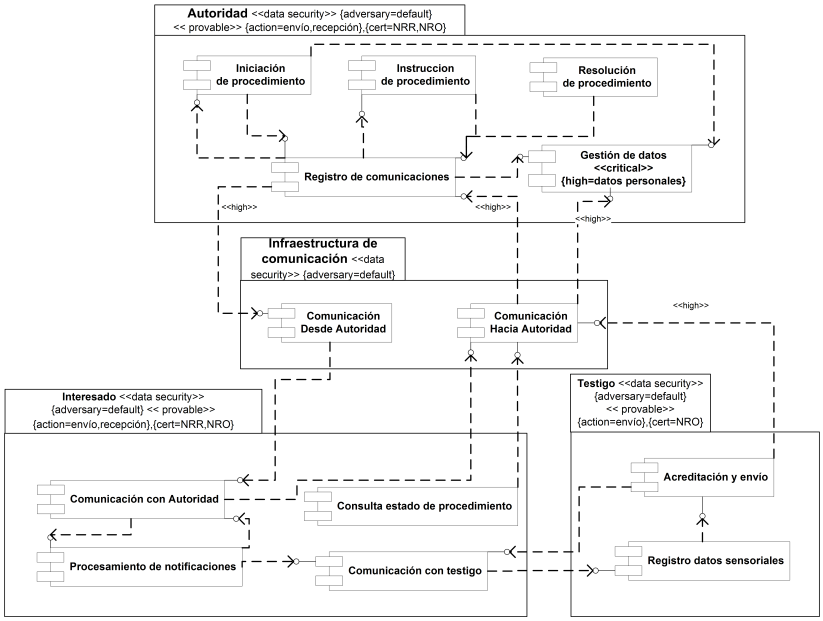

Figura 2. Modelo propuesto de proceso sancionador electrónico en el ámbito del control del tráfico

A diferencia de lo que ocurre en el modelo SIT de referencia (introducido en la Sección III), esta notificación se envía directamente a los interesados (entre ellos, el conductor sancionado). Dicho envío se efectúa a través del registro, quedando reflejado de nuevo en la infraestructura de almacenamiento. Para hacerlo llegar al interesado se emplea el componente de Comunicación desde la Autoridad.

La notificación recibida es interpretada en el componente de Procesamiento de notificaciones, el cual informa al conductor y evalúa la conveniencia de construir las pruebas electrónicas que sustentarán las alegaciones. Los datos que se utilizan para elaborar dichas pruebas proceden de los datos sensoriales (posición, velocidad, dirección, etc.) percibidos por los testigos. Una vez preparada la alegación se envía al componente encargado de la Instrucción del procedimiento a través del componente de Comunicación hacia la Autoridad. Nuevamente, el Registro electrónico se encarga de atestiguar la recepción de las alegaciones y de incorporarlo al expediente electrónico.

El componente de Instrucción del procedimiento valora entonces las alegaciones. En este punto, podría ser necesario realizar pruebas adicionales, como por ejemplo verificar el estado físico del registro de datos sensoriales del testigo iniciador del proceso. En ese caso, el proceso electrónico queda detenido a la espera de la necesaria intervención humana. En caso contrario, a la vista de las alegaciones se establece una propuesta de resolución, que es nuevamente enviada a los interesados del mismo modo que la anterior notificación. El vehículo, nuevamente, interpreta el mensaje recibido e informa al conductor, permitiendo que éste pueda conocer el estado del procedimiento de forma inmediata.

El proceso finaliza con la Resolución del procedimiento. A diferencia de los pasos anteriores, este componente participa en el proceso sin que sea necesario que reciba un mensaje. Esta resolución establece la sanción definitiva, para lo que se debe valorar toda la información contenida en el expediente. En caso de que se hubieran realizado pruebas que interrumpieran la instrucción electrónica del procedimiento, esta fase no podría automatizarse, puesto que la valoración de una prueba tradicional no es computacionalmente alcanzable, al menos a corto plazo. En caso contrario, este procesamiento se efectúa de forma electrónica, enviando a los interesados la notificación resultante. Dicha notificación es finalmente interpretada y su contenido comunicado al conductor.

IV-B. Análisis de seguridad del modelo propuesto

Para que el modelo propuesto tenga cabida en el actual marco legal es necesario satisfacer, al menos, los requisitos de seguridad impuestos por la legislación aplicable (presentados en la Sección II). En esta Sección se describen las necesidades de seguridad que afectan a cada una de las partes del modelo propuesto. Estas necesidades se han incorporado, en la medida de lo posible, en la Figura 2 mediante la extensión UMLSec [6]. Adicionalmente, aquellas que no tenían cabida en dicha extensión se describen en el texto a continuación. Por claridad, se explicarán separadamente los requisitos que afectan a cada uno de los subsistemas que conforman el procedimiento: Autoridad, Infraestructura de comunicación, Interesado y Testigo.

Antes de comenzar la explicación, es necesario caracterizar al adversario frente al que hay que satisfacer las necesidades de seguridad. En el modelo actual se ha escogido el atacante definido por defecto en [6]. Dicho atacante es de tipo externo y puede borrar, leer e introducir mensajes en un canal inseguro, así como borrar datos de un canal cifrado. Este modelo de atacante es razonable para el modelo propuesto, pero debe ser adaptado y extendido en función de la arquitectura que se

derive posteriormente.

IV-B1. Subsistema Autoridad: Este subsistema necesita incorporar la seguridad adecuada para la tramitación del expediente electrónico. Debido a la naturaleza de los datos en juego, es necesario proteger su confidencialidad, lo cual se refleja con el estereotipo *data security*. Por otra parte, se debe evitar que en este subsistema se pueda negar que se envió o recibió una cierta información. Por este motivo, este subsistema tiene el estereotipo *provable*, que se aplica a ambas direcciones del intercambio de información.

En lo que se refiere a necesidades específicas de algunos componentes, el de gestión de datos tiene el estereotipo *critical* dado que alberga todos los datos relativos a los expedientes. Dichos datos son, por su naturaleza, críticos para el procedimiento, por lo que deben extremarse las precauciones en cuanto a su preservacion. Por otra parte, el registro electrónico necesita asegurar su disponibilidad para estar permanentemente accesible.

Finalmente, las dependencias existentes entre este subsistema y los restantes se han marcado con el estereotipo *high*, que refleja que los datos intercambiados son de naturaleza altamente sensible, por lo que deben eliminarse los riesgos de acceso, modificación y borrado no autorizados que puede realizar el atacante considerado.

IV-B2. Subsistema Infraestructura de comunicación: Este subsistema ejerce de intermediario entre el subsistema Autoridad y los demás subsistemas. Se trata por tanto de un subsistema crítico en el conjunto del proceso y por ello se exige su máxima disponibilidad. La transmisión que efectúe este subsistema debe proteger la información en los mismos términos en los que se exige en los demás subsistemas. Por este motivo, se impone a este subsistema el estereotipo *data security*. Debe notarse que éste impone, además, la confidencialidad, integridad, autenticidad y frescura de dichos datos. A diferencia de los demás subsistemas, éste no envía ninguna información por sí mismo, sino que sólo retransmite aquellas que recibe. Por este motivo, en este subsistema no se impone el estereotipo *provable* para la envío de los datos. Igualmente, tampoco se exige para su recepción, puesto que no es el destinatario final de ninguno de los mensajes intercambiados. Sin embargo, sí se exige la auditabilidad de su funcionamiento, a fin de poder verificar (a posteriori) la corrección de su funcionamiento.

IV-B3. Subsistema Interesado: Este subsistema recibe los datos correspondientes al procedimiento y, en su caso, envía las alegaciones a la Autoridad. Dada la sensibilidad de la información en juego, este subsistema se ha marcado con el estereotipo *data security*. Además, debe quedar constancia de la fecha y hora en que se recibe y se procesa la notificación, pues este dato es relevante en el proceso sancionador, tal y como se expuso en la Sección II. Igualmente, no debe poderse negar el envío de las alegaciones. Ambas necesidades se reflejan con el estereotipo *provable* sobre ambos intercambios de información.

Además de lo anterior, sobre este subsistema debe satisfacerse el requisito de disponibilidad, pues puede recibir potencialmente numerosas notificaciones en un corto espacio de tiempo.

IV-B4. Subsistema Testigo: Este subsistema necesita asegurar los datos que gestiona, pues contienen información de carácter personal (por ejemplo, la identidad del supuesto infractor). Esta necesidad justifica el uso del estereotipo *data security*. Por otro lado, el testigo no debe poder negar el envío de la solicitud de iniciación del procedimiento. Esto se refleja mediante el uso del estereotipo *provable*.

La exigida autenticidad de los datos recogidos por el testigo se traduce en dos necesidades interrelacionadas. En primer lugar, los datos sensoriales recogidos deben ser veraces, es decir, reflejar fielmente la realidad. En segundo lugar, dichos datos deben estar referidos al comportamiento de un vehículo convenientemente identificado y autenticado. Esta última necesidad debe satisfacerse sin comprometer la debida privacidad de los conductores. Así, dicho componente, exclusivamente en el caso de que exista infracción, debe obtener el conjunto mínimo de datos para identificar al vehículo y, deseablemente, al conductor. De lo contrario, podría seguirse la trayectoría de un vehículo a lo largo de las carreteras. Dicho seguimiento constituye una violación de la debida privacidad del conductor incluso si solo se identifica al vehículo, en tanto que habitualmente existe una relación entre el vehículo y su conductor. Dicha relación permite que la identificación del vehículo se convierta, indirectamente, en la de su conductor [7].

Además de lo anterior, el testigo debe ser auditable, manteniendo un registro de sus acciones que permita verificar su correcto funcionamiento. Finalmente, el testigo debe estar plenamente disponible, tratando de maximizar la cantidad de observaciones procesadas por unidad de tiempo.

IV-C. Análisis preliminar de viabilidad técnica

El modelo propuesto identifica las principales funciones que permiten abordar de manera electrónica el procedimiento sancionador. Sin embargo, la implementación práctica de dichas funciones queda fuera del alcance del modelo. En esta Sección se introducen algunas tecnologías que pueden ser de interés para abordar esta implementación, satisfaciendo los requisitos de seguridad identificados en la Sección IV-B. Si bien el subsistema Autoridad puede desarrollarse utilizando técnicas de computación más tradicionales, los restantes parecen requerir un enfoque más innovador, pues se implementan en un entorno distribuido donde el vehículo cobra una mayor importancia. A continuación se explican las técnicas que se han identificado en primera instancia como relevantes para el futuro desarrollo del modelo.

Para el desarrollo del subsistema de Infraestructura de comunicación, se pueden aprovechar las diversas tecnologías identificadas por el proyecto CVIS[2]. De entre estas, destacan las alternativas basadas en satélites y las que aprovechan los recientes desarrollos en materia de comunicación vehicular (redes VANET, introducidas en la Sección III). En esta última alternativa, se exige el despliegue de una infraestructura de

[2]http://www.cvisproject.org/

comunicación a lo largo de las carreteras denominada RSU (del inglés *Road-Side Unit*, unidad de comunicaciones longitudinal a la vía). Una de las principales ventajas de su uso es que se permite una comunicación directa y permanente con el vehículo, donde podría alojarse el subsistema Interesado. Para asegurar la conectividad, los vehículos se equiparían con los dispositivos OBU (del inglés *On-Board Unit*, unidad de comunicaciones a bordo). Este tipo de comunicación vehículo-infraestructura dispone de su propia norma acerca de la seguridad de las comunicaciones (IEEE 1609.2, [8]), la cual será de interés a la vista de los requisitos identificados en este trabajo.

Con respecto al subsistema Interesado, se necesita disponer de una plataforma de computación que proteja tanto la información en juego como la corrección de su procesamiento. A este respecto, los dispositivos HSM (del inglés *Hardware Security Module*, módulos de seguridad físicos) satisfacen las necesidades planteadas en el modelo [9].

Finalmente, con respecto al subsistema Testigo, resulta necesario disponer de técnicas confiables de percepción del entorno. Con este fin, los dispositivos EDR (del inglés *Event Data Recorder*, registrador de eventos) permiten registrar lo ocurrido en el entorno vehicular. Además, con el fin de poder incorporar en una visión única las percepciones de varios testigos, se pueden utilizar (o adaptar) protocolos que evalúan la credibilidad de cada uno de ellos [10]. Además, de cara a asegurar los propios sensores y la transmisión de información, pueden aprovecharse los mecanismos propuestos por proyectos de investigación, tales como OVERSEE[3].

V. Trabajos relacionados

Las principales contribuciones técnicas relativas al procedimiento sancionador electrónico en el ámbito del control del tráfico han buscado mejorar la recepción de información por parte del ciudadano. Así, en el caso de España se han implementado las notificaciones telemáticas referidas al tráfico, en las que se envía un mensaje al teléfono móvil advirtiendo de la recepción de una notificación electrónica en la Dirección Electrónica Vial[4]. El modelo propuesto traspasa los límites de esta iniciativa, permitiendo que no sólo se reciba información sino que también se puedan aportar datos al procedimiento.

Por otro lado, el procedimiento sancionador de tráfico se ha modificado recientemente en España [11]. Dicha reforma busca acortar los plazos de tramitación eliminando la fase de instrucción para aquellos conductores que accedan a pagar el importe de la sanción inicial. El modelo propuesto en este trabajo supera a dicha reforma, en tanto que conjuga de una manera razonable los intereses de ambas partes: la Administración desea evitar que los procedimientos se alarguen, pero el ciudadano tiene derecho a defenderse en situación de igualdad probatoria. Para la creación de estas pruebas en el entorno vehicular, existen propuestas previas que pueden servir de base para el desarrollo de la arquitectura derivada del modelo presentado en este trabajo [12].

[3]https://www.oversee-project.com/index.php?id=9

[4]http://www.dgt.es/portal/es/oficina_virtual/multas/notif_por_internet_movil/

VI. Conclusiones y líneas futuras

El procedimiento sancionador permite la imposición de castigos a aquellos ciudadanos cuyo comportamiento no sea acorde con la Ley. Sin embargo, su implementación actual sufre de una excesiva burocracia que redunda en una menor transparencia, eficacia y eficiencia. En este trabajo se ha descrito el procedimiento sancionador y su realización electrónica según la legislación vigente. Partiendo de este marco, se ha propuesto un modelo para su aplicación en el ámbito del control del tráfico con especial atención a los aspectos de seguridad necesarios. Hasta donde se ha desarrollado esta investigación, esta es la primera propuesta que plantea la realización electrónica de todas las fases del procedimiento, lo cual constituye un punto de partida para su tramitación íntegramente automática. El modelo propuesto persigue fundamentalmente incorporar dos características novedosas a las propuestas previas: alcanzar una comunicación directa con el interesado y permitir que éste pueda crear pruebas electrónicas que sirvan de base para las alegaciones. Con ello se persigue proporcionar un conocimiento inmediato del estado del procedimiento a los implicados y otorgarles una mayor capacidad de intervención en el proceso.

Las líneas futuras de trabajo se centran en desarrollar una arquitectura derivada del modelo propuesto, tomando como base las técnicas que se han identificado de forma preliminar en este trabajo.

Agradecimientos

Este trabajo ha sido parcialmente financiado por el Ministerio de Ciencia e Innovación (España), dentro del Plan Nac. de Investigación Científica, Desarrollo e Innovación Tecnológica 2008-2011, contrato TIN2009-13461 (proy. E-SAVE).

Referencias

[1] España. Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos. *Boletín Oficial del Estado*, 23 de junio de 2007, núm. 150, pp. 27150-27166.

[2] España. Ley 30/1992, de Régimen Jurídico de las AA. PP. y del Proc. Admin. Común. *Boletín Oficial del Estado*, 27 de noviembre de 1992, núm. 285, pp. 40300-40319.

[3] L. Le *et al.* CAR-2-X Communication in Europe. En: S. Olariu; M.C. Weigle (eds).*Vehicular Networks: From theory to practice*. CRC, 2009.

[4] Parlamento Europeo. Resolución legislativa por la que se establece el marco para el despliegue de los sistemas de transporte inteligentes en el sector del transporte por carretera. Estrasburgo, 2009.

[5] R. Bossom. *European ITS Framework Architecture, Functional Viewpoint, Version 3*. Proyecto FRAME-S, 2004.

[6] J. Jürjens. *Secure systems development with UML*. Springer-Verlag, 2005.

[7] J. M. de Fuentes; A.I. González-Tablas; A. Ribagorda. "Autenticacion y privacidad en redes vehiculares". En: *Novática*, núm. 202, 2010.

[8] IEEE. *Trial Use Std. for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages*. 1609.2. IEEE, 2006.

[9] J. Attridge. *"An overview of Hardware Security Modules"*. SANS, 2002.

[10] N. Lo; H. Tsai. "Illusion attack on VANET applications - A message plausibility problem". En: *Globecom Workshops*. IEEE, 2007.

[11] España. Ley 18/2009, por la que se modifica el texto articulado de la Ley sobre Tráfico, Circulación de Vehículos a Motor y Seguridad Vial. *Boletín Oficial del Estado*, 24 de noviembre de 2009, núm. 283, pp. 99594-99624.

[12] J. M. de Fuentes; A.I. González-Tablas; A. Ribagorda. "Witness-based evidence generation in Vehicular Ad-Hoc Networks". En: *Proc. 7th Embedded Security in Cars Conference (ESCAR)*, 2009.